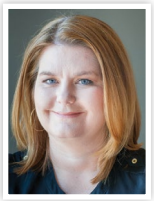
THE GLB ACT AND APPRAISALS

Visit WorkflowGeeks.com for more free titles.

TABLE OF CONTENTS

About the author



Jennifer Miller
President
Jennifer.Miller@MercuryVMP.com

Mercury Network

Jennifer is the president of Mercury Network. With 15 years experience in software development, transaction management, and workflow design, Jennifer guides the product development team, strategic partnerships, and growth strategies for Mercury. Jennifer was named a "2011 Innovator of the Year" from Progress in Lending Association, and was named a "Giant of Innovation" and a "Most Influential Women in Housing" by HousingWire.

Is your appraisal process breaking federal law?

Lenders are under more regulatory compliance scrutiny than ever, especially as consumers engage lawyers nationwide in foreclosure, valuation, and predatory lending lawsuits — many of which are turned into class actions. Unfortunately, some lenders are discovering that the way they order and receive appraisals is in violation of the GLB (Gramm-Leach-Bliley) Act.

The Gramm-Leach-Bliley Act, passed in 1999 and fully effective in July, 2001, addressed overall financial industry reforms as well as emerging consumer privacy and security issues. Officially called the "Financial Modernization Act of 1999", it affects the technology policies used by anyone engaged in providing financial services either directly or indirectly to consumers.

The Act regulates how consumer information is handled, and specifically addresses appraisals. **If appraisals are ordered or received using regular unencrypted e-mail, or even via fax machines in an open unsecured area, then GLB is being violated,** since those contain consumer data that GLB mandates as protected. If sales contracts are attached to appraisal orders and reports, then it's even worse. And storing printouts of those documents in cardboard boxes or unlocked file cabinets is strictly forbidden. Every day, many lenders are subjected to every one of those risks.

A consumer privacy breach can be exceptionally expensive, and everyone in the transaction can get mired in the ensuing legal liability mess. With consumers more militant and better armed than ever, most lenders are one non-shredded trash bin or accidentally forwarded e-mail away from a privacy lawsuit.

The good news is that technology can help you mitigate these risks. Lenders need a fully GLB-compliant solution, with end-to-end encryption, a secure upload/download container for sales contracts and other sensitive documents, appraisal PDFs that are never directly attached to e-mail messages, and secure paperless storage of transaction documents.

If you use an AMC, you're not automatically out of the woods. Many AMCs use non-secure processes either internally or with the appraiser, loan officer, or real estate agent. And under the GLB's "Safeguards Rule", the lender is responsible for the actions of suppliers to whom the consumer's private information is entrusted. If they aren't 100% GLB compliant, then the lender isn't either, and GLB holds the lender legally liable for not auditing the practices of business partners. Think of it as "SAS-70 with a $100,000 fine per audit violation plus a prison option". It's not a pretty picture.

Use this guide to help your organization identify risks and put measures in place to protect your borrowers, your suppliers, and your organization. **Feel free to call us at 1-800-434-7260 or send an e-mail to info@MercuryVMP.com for more information and for answers to all your appraisal questions.**

INTRODUCTION TO THE GLB ACT

The Gramm-Leach-Bliley Act was passed in 1999 and fully effective in July, 2001. The Act addressed overall financial industry reforms as well as emerging consumer privacy and security issues. Officially called the "Financial Modernization Act of 1999", it affects the technology and information system policies used by anyone engaged in providing financial services either directly or indirectly to consumers. For the text of the full Act, visit the government's official copy here:
http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

Under GLB, both the security and the privacy of a consumer's **non-public personal information ("NPI")** are protected. Charged with implementing the act, the Federal Trade Commission addressed the security and privacy components separately by issuing two distinct rules, the **"Safeguards Rule",** and the **"Privacy Rule".**

Lenders, appraisers, and mortgage professionals are subject to the rules. All are required to implement at least the following:

- Under the Safeguards Rule, secure the transmission, receipt, and storage of data relating to any consumer's NPI at all times, via passwords, encryption, and physical protection, backed by a written information security plan
- Under the Privacy Rule, provide easily understood privacy statements to any consumers who engage the appraiser, lender, or mortgage professional directly, disclosing the gathering, sharing, and security of NPI data, as well as the methods the consumer may use to opt-out of sharing of the data with third parties

The Appraisal Foundation addressed these rules and their applicability back in 2001.

Compliance is not difficult, but it does require understanding of the rules and the methods available. This Best Practices document will hopefully provide lenders, appraisal managers, and anyone else involved with the ordering and receipt of appraisals, with information and ideas useful in implementing GLB compliance as part of their overall regulatory compliance strategy.

Note: For Mercury Network clients, we've provided specific details at the end of this document regarding how Mercury Network protects the NPI you send and receive using our tools. Clients of other appraisal vendor management platforms should contact their own vendors directly.

NON-PUBLIC PERSONAL INFO

NPI includes loan terms, lender or mortgage broker name, sales concessions, co-borrower, unpublished phone numbers, other contact information, and of course more sensitive information as well. Even the fact that a particular consumer is engaged with a particular lender, at the time of the appraisal, is considered to be NPI if it has not been recorded in the public record yet or disclosed in some other way.

Whether or not some of the data might eventually be disclosed post-closing through recording of deeds and mortgages is irrelevant. At the time it is provided, it must be treated as NPI and accorded all of the security and privacy controls under the law.

Perhaps more importantly, the burden is on the you to determine whether the data provided is public information or not. Whomever is transmitting the consumer information — the appraiser or the lender — is required to have a "reasonable basis to believe" that the data is publicly available. In other words, research must have been done to determine its public availability first. One could not assume that a phone number or an e-mail address is publicly listed without verifying it.

To be safe, anything about a particular borrower or individual, which is not absolutely known to be public at the specific moment you receive the information, should be strictly treated as NPI, and subjected to your implementation of both the Safeguards and Privacy Rules.

Best Practices

It's safest to simply assume that all appraisals contain NPI, and therefore, the Safeguards Rule precautions must be taken. The Privacy Rule also applies at all times, but the actions you must take vary depending on which institution the individual engaged directly.

It's also important to note that the appraiser, lender, or appraisal manager may not fall back on any state regulations which are less protective than the federal regulations. Only those state laws offering greater protection of the consumer's NPI, in the eyes of the FTC, are considered to apply. By way of example, California's OREA provided guidance on complying with GLB in its Winter, 2002 newsletter, available at this link: http://www.orea.ca.gov/pdf/CAv13n02.pdf.

INSTITUTION APPLICABILITY

GLB applies to financial institutions of all sizes. It also applies to appraisers, as your supplier defined under the Safeguards Rule. In addition, the Act also applies to appraisers through the Code of Federal Regulations [§ 4(k)(4)(F); 12 C.F.R. § 225.28] specific definition of appraisers as such: "A personal property or real estate appraiser is a financial institution because real and personal property appraisal is a financial activity listed in 12 CFR 225.28(b)(2)(i) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act."

Like all laws, opinions differ as to the level of applicability in particular circumstances (lawyers are, after all, paid to argue both sides). When evaluating whether or not a law applies, it's valuable to look at the intent of the legislators and regulators implementing it. In the case of GLB, the rules were submitted for industry comment by the FTC prior to adoption. The commission noted specifically that lenders requested specific waivers for the hundreds of thousands of appraisers, attorneys, and accountants in the settlement services chain.

The commission rejected the request, replying that the security of NPI must be maintained at every link in the chain and that lenders could not abdicate the responsibility of the Safeguards Rule at any point. The FTC considered the case of appraisal transactions specifically, and clarified in the public record that the rules do indeed apply to appraisers. Throughout the FTC's official business guides to the two rules, posted on its website, appraisers are specifically listed up front as being covered by each particular rule.

The FTC guidance is also very clear that size of the company is not an exception. A one-person appraisal shop is an "institution" under GLB and is bound by the law exactly to the same extent as any other institution.

It's important to note that the GLB rules apply to the institution, not the transaction, since the consumer's NPI is held by the institution and unrelated to a transaction's "federally related" status. A transaction also does not have to be successfully completed for the rules to apply. The consumer information merely has to be provided to any "financial institution" in the performance of financial services, such as appraising.

Just as FIRREA resulted in the creation of USPAP, the GLB act resulted in the creation of the Safeguards Rule and the Privacy Rule. Both are sets of rules created by federal agencies as a direct implementation of federal law, and both are non-optional in any overall regulatory compliance obligations.

The practical application of the two rules can be summarized this way:

The Safeguards Rule always applies to appraisers and appraisal managers, whether with an appraisal management company or inside a lending institution. A consumer's NPI must be securely handled at all times, regardless of where it originated, how it is held, or what type of transaction prompted it.

The Privacy Rule only applies when the institution (appraiser, lender, et al.) is directly engaged by an individual consumer.

Best Practices

At the bare minimum, all transmissions with NPI, including the order and the final appraisal, must be via secure methods.

Realize that USPAP is talked about frequently among appraisers because it guides numerous individual valuation decisions, on a daily basis. But GLB similarly guides numerous individual data handling decisions, especially as related to e-mails to and from appraisers, appraisal management companies, and lenders, on orders and final reports.

As an analogy, most of us have encountered privacy hurdles attached to medical information under HIPAA. Medical providers, from dentists to insurance companies, are now required to provide additional disclosures to patients, cannot provide information even to other family members, and must provide checks and balances even in person to ensure only authorized access is granted to information. It changed everything related to how privacy of medical information is implemented. It affected virtually every aspect of any medical provider's daily interaction with the public, from phone calls to e-mails to paper storage.

GLB is effectively the financial counterpart to HIPAA, and its impact on even the most low-level tasks conducted in real property valuation should be considered no less sweeping.

INSTITUTIONAL RISKS

Kansas-based Nations Title Agency was caught with discarded loan applications in its (unsecured) dumpster in 2005, and was also investigated by the FTC for other alleged privacy violations. A news account of the resulting settlement appears here.

The FTC's complaint against Nations Title, here: http://www.ftc.gov/os/caselist/0523117/0523117NationsTitleComplaint.pdf, is sobering evidence of its expectation that third party vendors in the mortgage loan process — everyone in the "chain of custody" of personally identifiable information — have safeguards and compliant security policies. Nations Title will be required to, among many other things, obtain third-party assessments of its ongoing compliance with GLB standards and submit them to the FTC for the next 20 years. The settlement agreement is here: http://www.ftc.gov/os/caselist/0523117/0523117NationsTitleAgreement.pdf.

Clearly, this is an era of substantial litigation with respect to privacy and security of data, in all industries. There are also increasingly broad state and federal investigations of specific mortgage-related fraud activity.

While GLB does not provide a private cause of action, meaning individuals cannot personally sue for privacy violations, the FTC will investigate and will act on complaints. The GLB Act also gives authority to eight Federal agencies and the states to administer and enforce, making it a broad sweeping effort and on the radar or several enforcement agencies. As foreclosures continue, and lawyers for both consumers and lenders get involved, an environment is created where threatened GLB complaints to the FTC become settlement leverage in valuation disputes.

Best Practices

GLB-related liability is always present. Don't increase legal exposure by ignoring it. Compliance is much easier than it appears on the surface, and much easier than responding to an investigation or lawsuit after the fact.

As always, consult your own legal advisors. This document is not intended to provide legal advice of any kind. It is merely our opinion of selected technological best practices for GLB compliance. Simply put, if we were in your shoes, this is what we would do.

GLB AND COMPLIANCE PLANNING

GLB has been in force since mid-2001, so it isn't new. But with the combination of the mortgage boom and the post-bubble regulations, GLB compliance took a back seat at most institutions, large and small. Recently however, with foreclosure procedures and mortgage fraud both capturing headlines, it's important to pay attention to GLB. As a provider of technology products directly to mortgage lenders, we were naturally asked by our clients to carefully research GLB and ensure that our technology is fully compliant.

In the process, we were surprised to find the clear references to appraisals and the lack of exceptions to the rules. We are now aware that many lenders and appraisal management companies are not in compliance, so we feel we are obligated to notify the industry of the relevant issues and to help anyone transition their businesses to practices consistent with the law. GLB compliance is therefore now an integral part of our overall compliance support.

Safeguards Rule: Security and custody of consumer data

The Safeguards Rule requires that financial institutions implement written security procedures to prevent NPI from falling into the wrong hands. The complexity and scope of the written protocols may be appropriate to the size of the institution, but core security of the NPI may not be abdicated. NPI must be secured using passwords and encryption during any sort of transmission, as well as during storage (and physically secured even when stored in paper form).

All institutions are required to respect the sensitivity of the NPI data in all phases of a transaction, and interact with service providers appropriately, according to their written information security plan. This written information security plan and the relevant protocols in it must be referenced in the privacy policy provided to the consumer. The privacy policy should be provided by the party directly engaged by the consumer.

NPI data is potentially received electronically under many scenarios:

- Receiving an appraisal order via e-mail
- Receiving sales contracts and other financial documents
- Transmitting final appraisal reports to a lender (either a lender, appraisal management company, appraisal manager, et al.)
- Ad hoc e-mails with other service providers – agent, mortgage broker, loan officer, et al.

In addition to unauthorized access, the data must be secured from loss due to environmental hazards such as floods, as well as from technological hazards such as system failures.

GLB AND COMPLIANCE PLANNING

Obviously, you must implement secure means of sending and receiving documents containing NPI. Utilizing regular e-mails with NPI data in the message body or attachments, and even with password protected PDFs, is not sufficient. (Appraisers of course normally send a final report PDF with a password preventing a client from editing the PDF, to prevent fraud. But that still does not prevent anyone else from reading the PDF with the NPI in it. Access to the data is undeterred by preventing the editing of the report.)

Best Practices

Adopt a "custodial" mindset on all NPI data received, thinking in terms of security as well as preservation. Develop a written information security plan and have it on file at all times, and review it regularly. The plan must specify steps used to secure any communications containing NPI. The easiest method is by using password-protected website delivery over SSL (Secure Sockets Layer).

Obviously, each institution will adopt different levels of implementation. But at its core, NPI data must be secured at all times.

There may be cases of course where the appraiser receives no NPI, and therefore, in hindsight, encryption would not have been necessary. It would be tempting for an institution to decide therefore that security overall is not needed until the presence of NPI is certain. However, the institution would not be aware of the scope of NPI until the data had already been received, which would already be a security breach if NPI was indeed present. The only safe route is to assume that NPI is present and secure all communications appropriately.

Note that encrypted e-mail may also be used, but is more difficult to implement, since encryption keys must be exchanged manually with multiple providers. It's unlikely that most people will have encryption enabled in their e-mail at all. But all recipients and transmitters of NPI in the transaction are likely to be able to click a link to an SSL-enabled website in an automated e-mail, and to be able to set up password protected accounts on that site.

Regardless of the scope and type of encryption methods and processes used, developing a written security plan describing them is not optional. The law specifically requires that it be written and regularly reviewed. The institution must have it on file, and the privacy statement must refer to its presence.

Privacy Rule: Policy statements and opt-out provisions

Under the Privacy Rule, individuals fall into two categories: "consumers", and "customers". Consumers are any individuals who engage the institution at least once. Customers are simply consumers who have an ongoing relationship with the company. Both must be given privacy statements regarding the use of their NPI, and opt-out notices at specific times and circumstances, by the institution they engaged.

That last phrase is essential. When a lender or other business client provides the appraiser with NPI on an individual as part of a transaction, the appraiser is not required to provide another privacy policy disclosure to the individual. The appraiser's client must ensure that the suppliers it engages are in compliance with the privacy disclosures and opt-out notices it already provides to the individual.

Best Practices

The obligation to provide a privacy notice is on the institution whom the consumer directly engages. Appraisers should not send additional privacy notices to consumers brought by a lender or other institution.

Typically, an appraiser does not share the NPI with any non-affiliated third parties except where required to process the report. Appraisers don't usually sell or otherwise distribute their databases for marketing purposes. Most appraisers should be able to invoke the exceptions to opt-out notification as provided in sections 313.13, 313.14, and 313.15 of the act.

Your institution's privacy statement needs to address how the NPI will be handled and disclosed (if at all), how the consumer may opt out, and how the data is safeguarded.

The latter is why the company's individual safeguards policy must be in writing. The privacy statement does not need to include the full text of it, but it does need to state that the procedures are in place and are in writing.

GUIDANCE FOR OUR CLIENTS

Choosing an overall approach

The important thing when evaluating your options is to scale them to your needs, and remember that it's not "all or nothing". Improving security and compliance is a path, not a destination. It will never be "done" because the risks and methods constantly change. Don't feel like you have to have it all done tomorrow. You don't. You do need to start, and be educated, however. Security and privacy issues are not going away, ever.

If you're a smaller lending institution, or a smaller appraisal management company, you can keep it simpler. If you're larger, the risk and the expected standards for privacy communications, security, and employee training are probably higher.

Knock out the highest risk elements first. Generally, in the Safeguards Rule, you're most likely to transmit or receive valuable NPI in the original appraisal order and in the follow up documents (contracts and such).

Any time you receive or handle a document with a credit card number, an electronic bank account number, a loan account number, or an SSN on it, you're handling the most sensitive data in the consumer's NPI, and the security and privacy standards go up accordingly. Since you don't know when you'll receive data that already contains something sensitive, it's usually a good idea to employ the strictest security all the time, up front, so that it's not "too late" by the time you see it.

That being said, you can apply different standards of security based on your beliefs of the risk. If, for example, you don't believe that digital faxes inside unencrypted e-mails pose a risk, approach that aspect last, or not at all. (But even eFax recognizes the non-compliance of unsecured faxes in e-mail and has a system designed specifically for GLB requirements: http://www.efaxcorporate.com/corp/twa/page/glb).

It's your decision as to what level of compliance you think is "reasonable", given your environment.

Don't forget that some state privacy laws are stricter than GLB's own Privacy Rule. The privacy statements and the opt-out provisions of GLB should be implemented no matter what when dealing with consumers.

Finally, remember that top-level privacy and security are good business, and appealing to your clients. If you decide to "lead the pack", tell them. Market yourself as being in full GLB compliance. Turn your efforts into profit instead of just an expense.

Complying with the Safeguards Rule using our products

To comply with the Safeguards Rule, security and safety of the data is necessary – inbound, outbound, and stored on your systems – and you must have a written security plan. The following are suggestions for using our products and others for compliance.

Develop a plan. Keep it simple at first – anything is better than nothing.

Send and receive appraisal orders securely. Avoid orders sent via regular Internet e-mail, as they can be intercepted and read easily (even attachments).

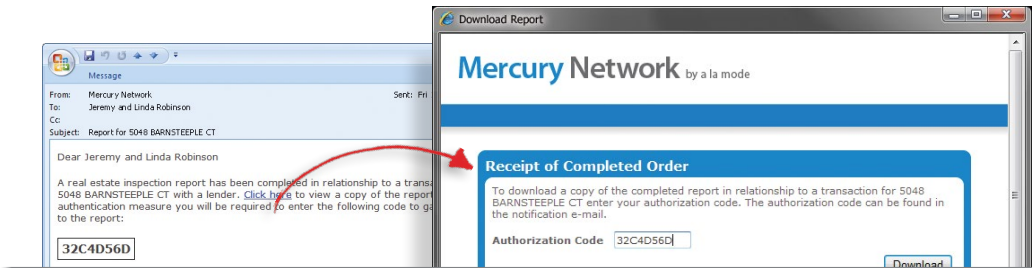
If you use Mercury Network, you can rest assured you have tools built in to protect you. Appraisals are delivered to you via Mercury Network's cloud-based platform and not through unencrypted e-mail. You must log in to the secure website with your password to access your appraisals. You will also receive all accompanying documents via Mercury Network, and avoid receiving them in unprotected e-mail.

If you are a lender or appraisal manager, place appraisal orders on a secure website like Mercury Network, and don't send accompanying documents as attachments via unprotected e-mail. Instead, upload them to the documents associated with your order inside Mercury Network for security, or send them via secure fax.

Send and receive all related documents securely. If you have related documents you want to attach to the appraisal, upload them to the documents section of your order inside Mercury Network. Do not e-mail them as attachments.

If an appraiser needs to fax something to you, ask them to use your DirectFax technology inside Mercury Network. When they click on the order, they can choose to upload a document via DirectFax to avoid using unencrypted e-mail attachments.

Send appraisals to your borrowers securely. Once the appraisal is complete, use Mercury Network's built in "Send to borrower" tool. It will send a professional e-mail to your borrower, alerting them that the appraisal is ready for them on a secure website. They must enter credentials to access the report.



Your borrower will automatically receive a notification e-mail with the URL for the secure website, and the password for downloading their report.

GUIDANCE FOR OUR CLIENTS

Complying with the Privacy Rule

To comply with the Privacy Rule, you have to deliver and display privacy statements as well as provide opt-out mechanisms to any consumer who engages you. Providing the privacy statements and opt-out methods is not optional. There are exceptions to the opt-out conditions when sharing that data with third parties, but not to the provision of the privacy statements up front.

Remember, the opt-out clauses only have an impact when sharing data with certain types of third parties.

Opt-out provisions may be stricter and more mandatory in some states (California, for example) than under GLB alone, so be sure you understand what other opt-out restrictions may be placed on you and try to incorporate those into your site as well. In any case, it's good business to have a strong, public-friendly opt-out policy.

- **Develop a privacy policy and opt-out mechanism.** Most lending institutions already have a privacy policy in place. If not, privacy policy examples are all over the web, on nearly every site you visit. Like the security plan, keep it simple at first – anything is better than nothing.
- **Post the policy conspicuously on your website.** It should be on the footer of every page, as well as in the main navigation. It should visually stand out. The law specifically requires that it be conspicuous.
- **Send your annual privacy policy statements en masse to all consumers you handled, as well as any time you change it.** By sending an annual statement to every consumer, you don't have to distinguish between "consumers" and the longer-term "customers". Also, send changed policies to everyone as soon as the change is made.

Most lending institutions are already doing this. But if not, the end of year is a great chance to thank borrowers for their business, and then also remind them of the policy and your high standards in handling their NPI. Use it as a marketing opportunity – not a sales pitch.

CONCLUSION

Mitigating risk and using best practices

We hope this guide has given you the information you need to develop a plan for your organization to better mitigate your compliance risks and protect your borrowers' privacy. As stated before, compliance with GLBA in terms of your appraisal desk isn't difficult. Knowing the laws is the first step, and adopting the right technologies can dramatically ease your compliance burdens, and even greatly enhance your efficiency at the same time.

If you have any questions, don't hesitate to contact us. We know these issues well, since the largest AMCs and lenders in the country rely upon Mercury Network to power over half the nation's residential real estate transactions. Give us a call today to go over your compliance needs and questions. You don't have to be a client of Mercury Network, and it could save your organization from serious penalties.

References

"Safeguards Rule" on the FTC's website:
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

"Privacy Rule", from the same FTC site:
http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html

Developing an information security program:
http://www.federalreserve.gov/boarddocs/SRLETTERS/2001/sr0115a1.pdf

Document from the California OREA, Winter 2002
http://www.orea.ca.gov/pdf/CAv13n02.pdf

Mercury Network

Contact us to get total control over your collateral valuation process. No implementation fees. No contracts. You have nothing to lose in trying it.

Visit www.MercuryVMP.com or call 1-800-434-7260.

Additional resources:

Free resources: Industry best practice guidelines and news
Get expert recommendations for compliance, efficiency, and maximizing profit.
www.mercuryvmp.com/resources/

WorkflowGeeks:
Get the latest in your inbox. Subscribe at:
www.workflowgeeks.com

Share this white paper with your colleagues: